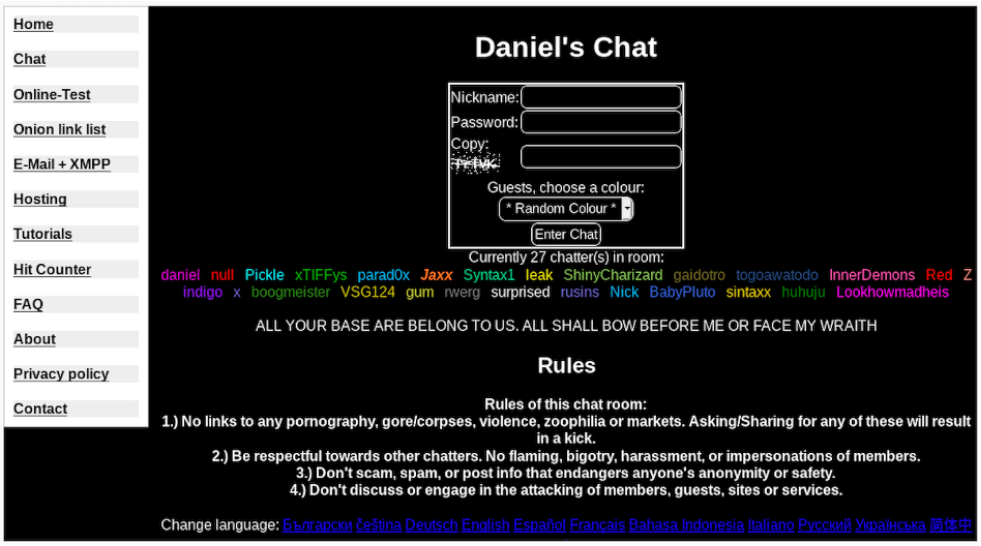
Daniel goes dark for good

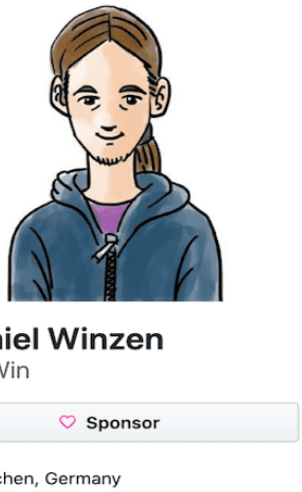
On March 10th 2020, hackers targeted one of the most prominent anonymous website hosting providers on the darknet, Daniel Winzen, subsequently knocking over 7,500 hidden services across Tor offline. DarkOwl analysts, who regularly monitor the darknet directly, observed this event occur via DarkOwl's Vision platform and have spent recent days reviewing what happened to quantify the impact to the darknet.

Editors note: the following report contains explicit language and references sensitive material.



Screenshot of Daniel's PHP chat during the recent March 10, 2020 hack

Who is Daniel Winzen?



Source: DanWin github user profile picture

Daniel Winzen, also known as "DanWin" or @daniel, has been a major player in the darknet community for at least the last five years. The German 20-something-year old has long provided hosting and directory services as well as e-mail and communication mediums like Jabber+XMPP and a PHP-based anonymous chat built on the LE code-based chat platform across Tor and I2p.

Winzen has been applauded by some for consistently providing the technical services he has, while others have criticized him for facilitating the distribution of illegal content from scammers and pedophiles.

Target: Daniel's Chat SQL Database

Around 01:00 UTC in the early hours of March 10th 2020, members present in Daniel's Chat were surprised to see their super admin, @daniel online. Since the last attack against Daniel's Hosting services in November 2018, @daniel rarely visited the chatroom, blaming member-infighting and a busy work schedule. It took no time to notice that the topic for the chatroom had been modified to "ALL YOUR BASE ARE BELONG TO US. ALL SHALL BOW BEFORE ME OR FACE MY WRAITH" [sic] and @daniel was not actually commanding his account in the chatroom.

A guest account, using the moniker @null was rapidly promoted to an administrator role, who kicked staff and members out of the chatroom and promoted another guest account with the moniker, @Pickle. The new admin, @null, had little to say, but did post an all-caps declaration positioning themselves "king" and demanding everyone "bow" to them.

"03-10 01:39:27 – null – I am your king now
03-10 02:15:04 – null – are you not going to bow before me? Your new leader
03-10 02:20:03 – null is now a registered applicant.
03-10 02:21:24 – null – I HAVE COME FOR YOU
03-10 02:23:49 – null – YOU SHALL ALL BOW BEFORE ME
03-10 02:27:13 – null – i have seized control over the chat;
03-10 02:28:35 – null – By the way, this chat logs your headers and has a backup of everything you say. You've all essentially been joining a honeypot.
03-10 02:31:52 – null – Also, daniel is no more
03-10 02:36:37 – Pickle is now a registered member.
03-10 03:46:42 – null – stick around
03-10 03:46:55 – null – You'll see the bigger picture soon"

— Excerpt from Daniel's Chatroom Transcript, March 10, 2020

Then, at 02:51 UTC, a chat user named @Dolly emerged without "entering," stating that the hackers stole @daniel's chat password and that the server itself had not been compromised. @Dolly also said, "*Doesn't look like you can delete @Syntax"* suggesting that @Dolly was likely an alternate account for the chatroom's controversial super administrator, @Syntax. She also confirmed that @daniel was not logged in as he was not usually awake this early to do so.

@Dolly's arrival prompted dialogue between the hacker @null and chatroom users, while @Syntax expressed less interest in fighting and was more interested in discussing the "reasoning" behind the hack.

At one point, @Dolly commends the alleged responsible parties by saying *"I'm kinda in awe as to what you did."*

"03-10 03:01:11 – Dolly – @null I see. I mean if that is what you wanted, I think that the parties running the chat would have handed it to you.
03-10 03:01:08 – xTIFFys – How so? @Z
03-10 03:00:54 – Z – chat got fucked
03-10 03:00:03 – xTIFFys – Hey. @meerkat
03-10 02:59:55 – null – I've downloaded everything I wanted.
03-10 02:59:52 – meerkat – Hakuna Matata =(^.^)= ❤ @xtiffys
03-10 02:59:37 – null – why not?
03-10 02:58:57 – xTIFFys – Hello everyone.
03-10 02:58:19 – xTIFFys entered the chat.
03-10 02:57:36 – Dolly – I won't fight you, I really would like to know the reasoning
03-10 02:57:16 – meerkat – Delete what
03-10 02:56:49 – Dolly – Why do you want to delete it?
03-10 02:56:28 – Dolly – @null. Okay.
03-10 02:56:12 – Dolly – What's the goal?
03-10 02:56:05 – null – I plan on deleting it
03-10 02:55:58 – null – No @Dolly
03-10 02:54:56 – anon – @null what do you mean this server is a honey pot
03-10 02:54:53 – Dolly – So this place in gonna turn back into a doxing, pedophile wonderland.

03-10 02:54:14 – Z – heh @meerkat
03-10 02:54:12 – Dolly – Thats how I know they don't have server access, they just have site access.
03-10 02:53:48 – meerkat – Someone should make me a mod so I can get a back door through the filters again
03-10 02:53:27 – meerkat – You need server admin to delete syntax 😂 nice try though
03-10 02:53:05 – Dolly – Its too early for daniel to be awake, in about an hour or so."

— Excerpt from Daniel's Chatroom Transcript, March 10, 2020

For the next hour, @Syntax along with various guests and transient members chatted about random subjects ranging from EU and German laws around pedophilia to the 19th Amendment, while random trolls entered and continued to attack only @Syntax directly. One chat member and presumed online boyfriend of @Syntax, known by the moniker @Fuggles, joined the chat and had little to say.

One guest to the chatroom suggested the hack was organized by @Syntax to breakup with @Fuggles, while another long-time user and former staff of Daniel's Chat, known as @meerkat simply hypothesized that the hacker @null and @Syntax were one and the same person – essentially alleging that this was orchestrated from the inside.

"03-10 03:36:14 – meerkat – I have a feeling @null is syntax.
03-10 03:36:19 – xTIFFys – I think that guy was strangled not shot. @anon
03-10 03:36:27 – meerkat – Actually if be willing to bet my next pay check
03-10 03:37:21 – xTIFFys – Wish I had that kind of security, @meerkat.
03-10 03:37:25 – xTIFFys – LOLZ
03-10 03:38:11 – meerkat – Hehe me too @xtiffys if I were to lose I'd be broke for a month"

— Excerpt from Daniel's Chatroom Transcript, March 10, 2020

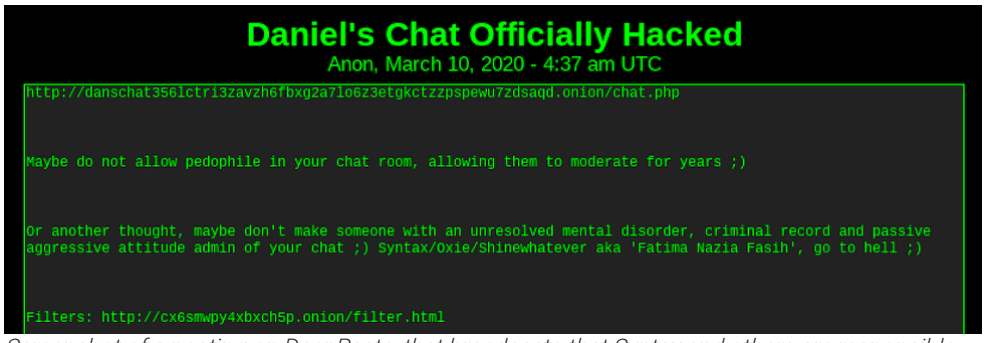
By 04:00 UTC, the hacker kicked @Syntax and all guests using variations of her nickname from the room. Less than 10 minutes later, @null stated Daniel's Chat was the last site left on Daniel's Hosting. This suggests that while everyone was conversing, the hacker/s were busy deleting the web services hosted on Daniel's servers by elevating the privileges of @daniel's admin account. We find this to be at least partially true as it appears that the hackers targeted Daniel's databases via the chatroom and not the web server content, like raw HTML and CSS files.

At 04:31 UTC, Daniel's account simply announced, "pwned." At 04:32 UTC, the chatroom returned displaying the message, "Fatal error: No connection to database!"- suggesting the hack was complete and the chat database was no longer online.

The method and the justification

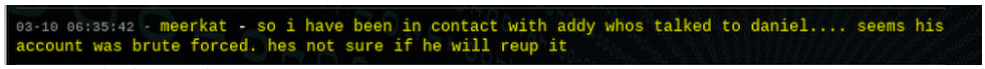
Less than 5 minutes after the chatroom went offline, a single post appeared on the drama and spam-filled Tor hidden service, DeepPaste, with the hackers blaming staff pedophiles and Syntax directly for the attack against Daniel's services. The hackers also included a link to another external hidden service on Tor with a list of all the filters from the admin panel in the anonymous chatroom. It is rumored staff moderators used the extensive list of filters, consisting of mostly keywords and URLs linked to illegal subject matter, for auto-kicking guests posting banned content.

The reason for posting this – along with their final statement – is unknown and the service containing the filters is no longer online.



Screenshot of a posting on DeepPaste, that broadcasts that Syntax and others are responsible for the takedown of Daniel's Hosting

A couple of hours after the hack, user @meerkat posted to another Le-Chat on Tor that he had confirmed with Daniel via his friend Adriane that his administrator password had been simply brute forced. Given @daniel's limited involvement, he expressed skepticism the chatroom would ever return.



Source: Black Hat Chat on Tor

The Hacker @null and the Accomplice @Pickle

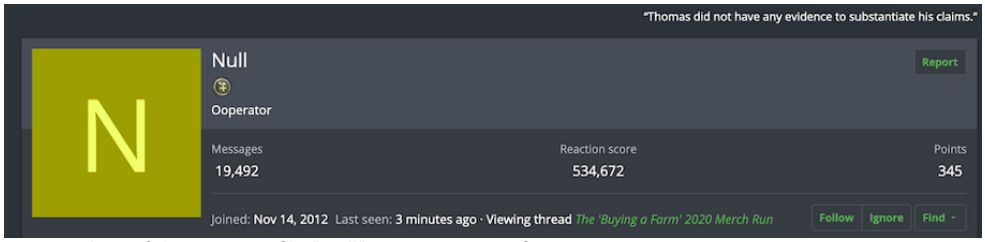
"03-10 04:07:28 – Pickle – Hmm, lots of people just seem to get what they deserve…
03-10 04:19:45 – Pickle – They're all against you.
03-10 04:20:10 – Pickle – They all must die…t"

— Excerpt from Daniel's Chatroom Transcript, March 10, 2020

Little is known about @null or @Pickle in the Daniel's Chat community, as the nicknames were not previously registered as members on the chat. While @null entertained questions from @Dolly/@Syntax about how the attack was conducted, @Pickle made only three statements over the last 30 minutes that the chat was online.

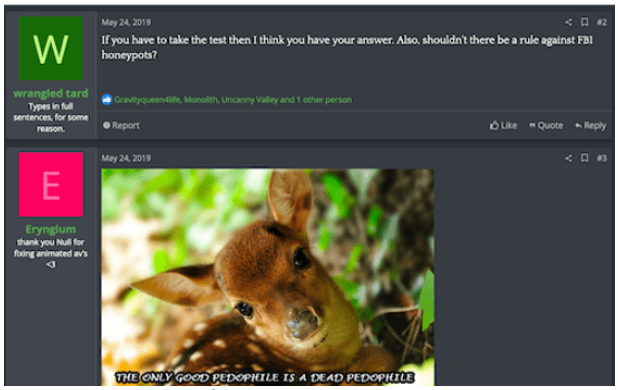
Using Vision, DarkOwl analysts uncovered lengthy history for both monikers (null and Pickle) in the underground community known as Kiwi Farms.

Kiwi Farms, formerly known as CWCki, has been on the surface web since 2013 and archived by DarkOwl on Tor since October 2017. It was set up by a Joshua "*Null*" Moon as an exclusive image board for trolling and harassing an autistic transgender web comic artist, but has since involved into a dedicated discussion board for "lolcows" including stalking and doxing of public and internet figures.



Screenshot of the user profile "Null" on Kiwi Farms forum

The content on Kiwi Farms is consistent with typical chanboard-like discussions. There are reoccurring anti-pedophilia threads and general disdain for FBI honey-pots. There are very few technology or hacking focused threads on the Kiwi Farms forum.



Source: Kiwi Farms forum

Source: Kiwi Farms forum

In November 2019, darknet hackers targeted Kiwi Farms leaking their member and conversations database on the popular forum, RaidForums, possibly giving the staff and members of the community at Kiwi Farms justification for a cyber-based retaliation.

https://raidforums.com/Thread-KiwiFarms-Database-Leaked-Download#kiwifarms#Users and Conversations#dna_jacked.16759-conversations-1.txt
Crawled on 2019-11-07 17:23:00 PM

```
[Nazi Isis Bravo Team of 30 +
TALES FROM THE CRIB 5106186](/conversations/nazi-isis-bravo-team-of-30-34
-cockless-mavericucms-threat-level-midnight-tales-from-the-
crib-5106186.44814/unread)
* __
* * [Y2K Baby](/members/y2k-baby.14836/)
* [000%](/members/000.32484/)
* [1864897514651](/members/1864897514651.15624/)
* [2odastream](/members/2odastream.19154/)
* [300mm](/members/300mm.10189/)
* [4acodmt](/members/4acodmt.33485/)
* [50'shousewaifuElvira](/members/50shousewaifuelvira.18818/)
* [666DEATHGAY](/members/666deathgay.35576/)
```

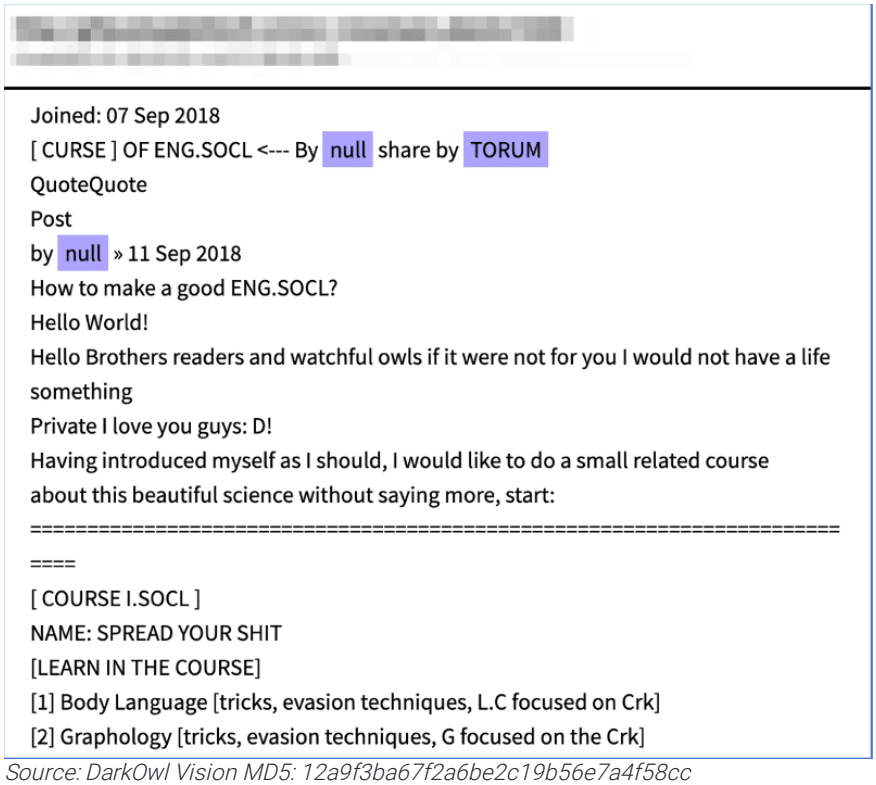
Source: DarkOwl Vision MD5 – 2e960aacf263ec00196320254f94ca1f

Despite the leak in 2019, the evidence connecting Kiwi Farms to the hack of Daniel's earlier this year is extremely weak and circumstantial. Kiwi Farms has over 50,000 registered users and several prominent members include "*Pickle*" in the moniker, e.g. long-time member "Pickle Inspector," but DarkOwl analysts were unable to connect these, nor their administrator "*Null*", to the hackers of Winzen's services.

Unfortunately, "null" is also a common moniker observed in recent years on popular darknet cybersecurity forum, Torum. In late 2018, "null" posted a course on social engineering, written as

CURSE OF ENG.SOCL.

The thread was not well-received, nor did the member "null" post that frequently, having less than a dozen posts on the forum since their registration in September 2018.



Joined: 07 Sep 2018
[CURSE] OF ENG.SOCL <--- By null share by TORUM
QuoteQuote
Post
by null » 11 Sep 2018
How to make a good ENG.SOCL?
Hello World!
Hello Brothers readers and watchful owls if it were not for you I would not have a life something
Private I love you guys: D!
Having introduced myself as I should, I would like to do a small related course about this beautiful science without saying more, start:
==========
====
[COURSE I.SOCL]
NAME: SPREAD YOUR SHIT
[LEARN IN THE COURSE]
[1] Body Language [tricks, evasion techniques, L.C focused on Crk]
[2] Graphology [tricks, evasion techniques, G focused on the Crk]

Source: DarkOwl Vision MD5: 12a9f3ba67f2a6be2c19b56e7a4f58cc

Did GhostSec send a warning a week prior?

On March 3rd 2020, a guest by the name of @Sebastian entered Daniel's Chat and stated "*GhostSec is watching you,*" adding that they had taken control of discord servers of Daniel's – servers that members in the chat didn't know he even had.

Shortly before getting kicked from the room, @Sebastian posted a fingerprint and claimed Daniel was compromised while accessing child pornographic content called, Tiny Voices. Sebastian is also the moniker and name of the leader of the anti-pedophilia hacking group formerly known as Ghost Security (#GhostSec). Sebastian Dante Alexander, who uses the Twitter handle, @SebastianDant13, is a vigilante hacker known for tracking and de-anonymizing criminals who harm children.

"03-03 19:08:15 – Sebastian – Daniel
03-03 19:08:44 – Sebastian – GhostSec is watching you
03-03 19:10:16 – Sebastian – Daniel I took ur discord servers and we are the ones eating these nodes
03-03 19:16:20 – Sebastian – 0d 6a a4 e8 45 b7 51 09 d5 c2 d4 39 fe 1f 69 5f 15 72 04 8c 40 48 74 dc b4 4f a1 ba ed e7 58 15
03-03 19:16:38 – Sebastian – That's his fingerprint we are tracking
03-03 19:16:44 – Dusted – hm?
03-03 19:17:12 – Sebastian – We have him for this pedo shit in Tiny Voices fucking Daniel the pedo left his fingerprint
03-03 19:17:32 – Sebastian – Uh oh
03-03 19:17:51 – Sebastian has been kicked."

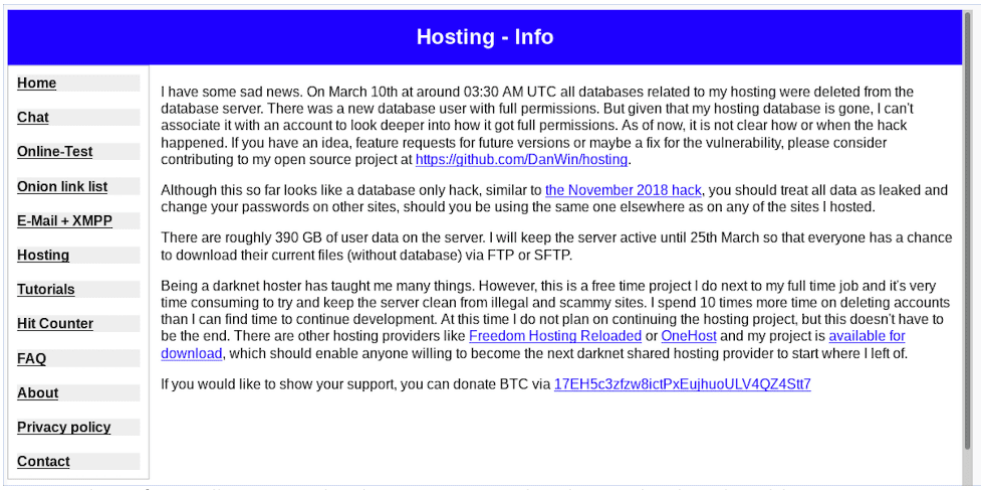
— Excerpt from Daniel's Chatroom Transcript, March 03, 2020

An organized hacking collective like GhostSec definitely has the capabilities and motivation to take down Winzen's servers, especially if there was questionable content hosted and shared, but the group has not published any declaration or claim of responsibility for the hack, like they have with other groups and individuals they've targeted in the past.

Daniel's response

As soon as Daniel was alerted to the hack, he posted a notification to his main website confirming what was suspected. The hackers deleted all databases related to his hosting platform and all users should consider their data leaked and passwords compromised.

He further stated the remaining 390GB of data from the websites he hosted would only be available until the 25th of March and recommended his customers use Freedom Hosting Reloaded or OneHost as he had no intention of restarting his hosting project.



Screenshot of Daniel's Hosting landing page immediately post hack with public announcement

Daniel followed up with an update on March 11th 2020, giving users more details on archiving what was left of their website data. Winzen referred to the flood of messages encouraging him to keep going with the hosting service, but Daniel stated that keeping his servers clean from scammers took time from development and projects he enjoyed. He left the option open, months down the road, but not until he found time to improve the current platform.

Update March 11th 06:00 AM UTC: Private keys of hidden services are now copied and available in your /data/ directory. If you don't know your system account to connect via (S)FTP, it consists of the first 32 characters of your first onion address. If it was a v2 address, it's the full address (including .onion). Since yesterday I've got several messages asking me not to give up. The project in it's current state is a lot of work to maintain. I have many ideas on what to improve and which features to add. But after spending most of my time on answering mails or getting rid of just another 50+ scam sites every day, there is hardly any time for development. I may start another hosting project in the future, when I found time to improve the current platform. But it may take several months before I get there.

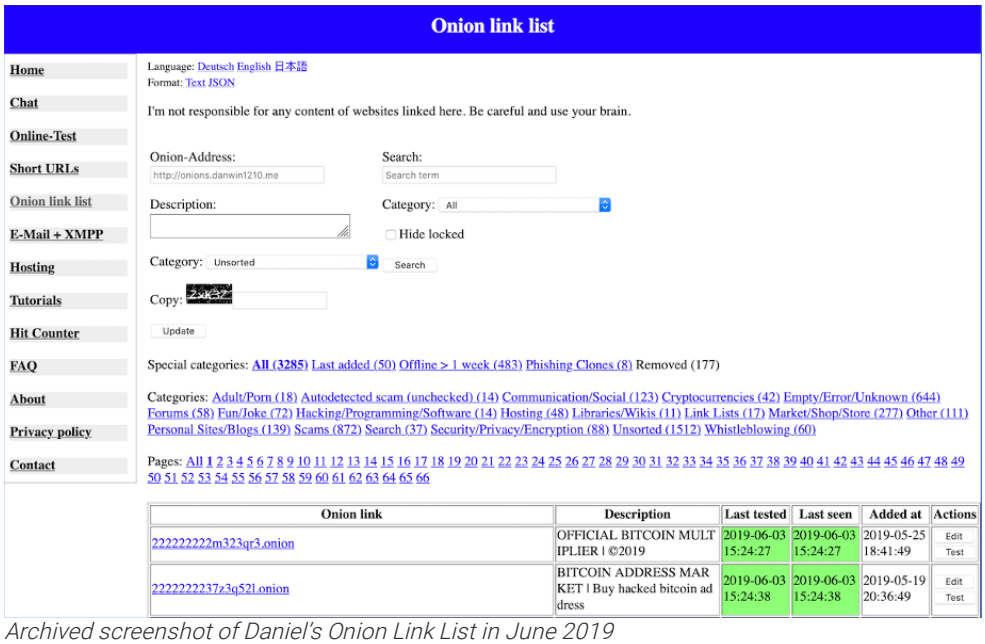
Response from @daniel regarding server status on March 11, 2020

No database backups

Speaking of server setup, strangely, Winzen did not maintain any archives of the SQL databases he hosted as evident by data loss, nor were backups of the deleted databases available when he was hacked previously in late 2018. Many darknet users have expressed increasing skepticism that Daniel was not as committed to his darknet projects as he would have liked everyone to believe. After the most recent database breach, one anonymous user suggested that @null's reference to the chatroom being a honey-pot was legitimate, adding suspicion over a server upgrade or move occurring only weeks before the most recent attack occurred.

Those who suspect that Daniel's chatroom was actually a honey pot surmise that Daniel didn't maintain backups of his data because they were being monitored (and probably managed) by international or German law officials. This was supported by the fact that a change in rule regarding sharing any pornographic content occurred in 2018, around the same time that Daniel was hacked and their databases disappeared.

There have been numerous pastes circulated around the darknet in the last year claiming many of the members, including @Syntax were Law Enforcement.



Archived screenshot of Daniel's Onion Link List in June 2019

Daniel's link list is lost

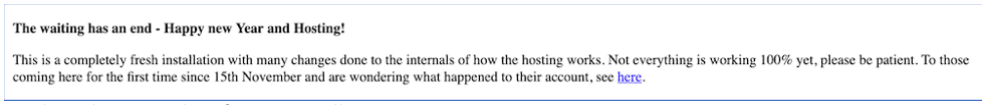
While the takedown of Daniel's Chat and Hosting have received significant attention, another item that was compromised during this time was Daniel's Onion Link List.

Winzen maintained a seed list of Tor hidden services, along with a status indicator and topical classifier that was helpful for those exploring the darknet regularly. This list of links was referred to by hundreds of other sites across Tor.

Now, Daniel's Onion link list returns a 504 Gateway Time-Out error.

DarkOwl analytical look

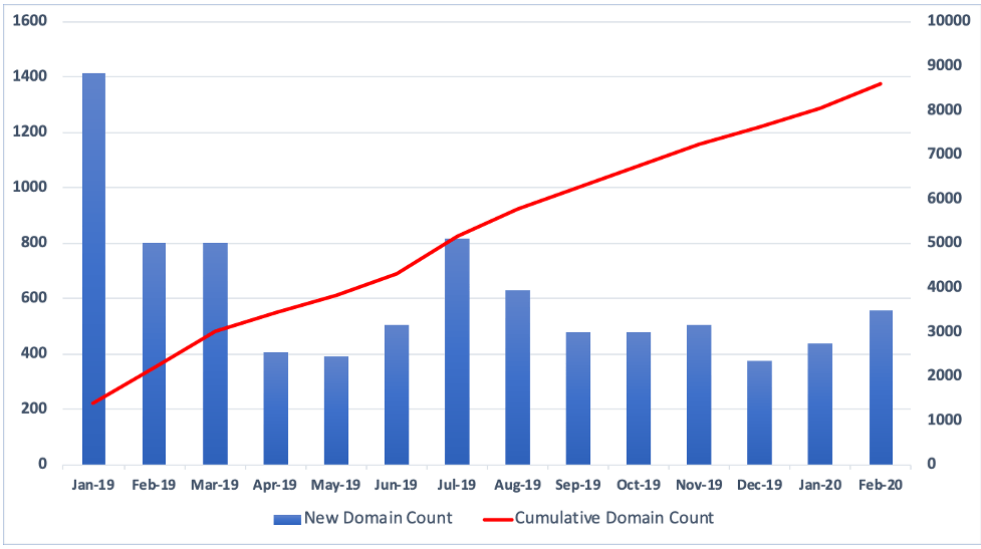
After the last hack in November 2018, it took Winzen almost two months to re-deploy his hosting services. On January 6th 2019, Winzen posted a happy new year and hosting message indicating his hosting services were back online.



Archived screenshot from Daniel's Hosting in January 2019

By January 10th, 2019, a mixture of over 1,400 darknet domains and subdomains appeared operational. This initial count of domains was determined by not only the domain name themselves, but careful review of the content of sites hosted by Winzen prior to and after the November 2018 hack.

Notably, DarkOwl Vision data shows an increase of over 7,600 domains affiliated with the hosting provider over the course of the 2019 calendar year.



Graph depicting number of domains tagged as Daniel's Hosting services via DarkOwl Vision

In DarkOwl's quantitative *Map The Dark* internal reports, domains are topically tagged as being associated with Daniel's hosting if, 1. The domain URL was discovered on the public "List of Hosted Sites" on Daniel's hosting or if, 2. The website contained the phrase "*Site Hosted by Daniel's Hosting,*" as has been observed with most newly published darknet hidden services. **As of March 9th 2020, DarkOwl had observed 9,006 domains or sub-domains affiliated with Daniel's hosting, 7,555 of which were recorded as online during the first two weeks of March 2020.**

Update March 13th 08:40 AM UTC: A data.tar.gz and www.tar.gz archive is now available in everyones home directory to speed up downloading by only having to transfer a single compressed file rather than a whole directory.

Update March 15th 10:30 AM UTC: All hidden services are now shut down to enable users to re-use the same address on a new host.

If you would like to show your support, you can donate BTC via 17EH5c3zfzw8ictPxEujhuoULV4QZ4Stt7

Update on Daniel's landing page on March 15, 2020

On March 15th 2020, Winzen once again updated his landing page to state that all hidden services were offline to make migration of his user's hidden service URL at a different darknet hosting provider. **By April 1st 2020, DarkOwl had identified approximately 1,200 hidden services topically tagged to Daniel's hosting as back (or still) online.**

DarkOwl analysts observed that many of the 1,200 hidden services consist of active sub-domains on Winzen's historical V2 onion URL (tt3j2x4k5ycaa5zt[.]onion). Most of the subdomains on the V2 onion URL first came online in June 2017, and have been consistently active to date. Many of these include offensive keywords, such as, pedohosting.tt3j2x4k5ycaa5zt[.]onion, and nazism.tt3j2x4k5ycaa5zt[.]onion. These are just a few examples of several dozen others that include similarly banned topics and offensive keywords.

These V2 domains simply re-direct to the V3 Tor landing page, and have never had web content available to publicly collect. Nevertheless, several of these subdomains contain illicit keywords that suggest Winzen might have been complicit with hosting illegal content, despite his rules and policies against such.

Interestingly, there are also another 43 subdomains starting with the string "password" and an additional 23 with the phrase "freedomhosting" or "freedomhostingnode" suggesting at one point, Winzen collaborated with long-time controversial darknet hosting provider, Freedom Hosting. Are these the "nodes" GhostSec was referring to on March 3rd?

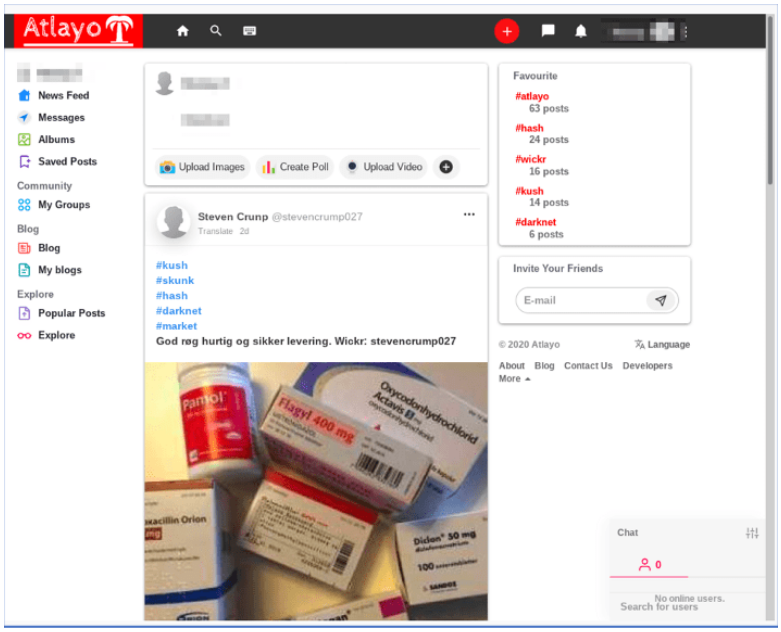
Currently, the V2 URL redirects to Daniel Hosting's V3 URL, which Winzen adopted after the November 2018 hack – presumably for enhanced security. Both domains have been referenced for his SMTP email domain by Winzen on his contact page. The Bitcoin addresses listed on Winzen's surface web mirror, danwin1210.me, and the Tor hidden service are different, but both have had numerous transactions since the hack occurred on March 10th, 2020.

The darknet will carry on

Despite Winzen's encouragement for his users to migrate their existing hidden services and URLs to other darknet hosting provider, most of the services didn't bother or adopted new URLs.

DarkOwl analysts reviewed over 5,000 URLs associated with Daniel's Hosting since the first of the year, to find less than two dozen had migrated and retained its URL as of early April 2020.

A long-time darknet Twitter-like social network called Atlayo (atlayofke5rqhsma[.]onion) is back online and operating using its previous URL, and it has long been rumored that Daniel was once a key moderator and administrator for this service.



Screenshot of current Atlayo sub-landing page

Security concerns over the once popular PHP-based LE-Chat platforms has more users migrating to IRC over Tor proxy, while those with hosting resources are offering up their web servers for hosting content in the interim. Users capable of web development have set up even more hidden services than they had while relying on Winzen alone, and clones of Daniel's home website are being advertised to ostensibly create a sense of familiarity and security.

One such example, OnionCommunity, online since the fall of 2019, has revamped with a layout shockingly similar to Winzen's. In addition to a chat (IRC), online link list and test, OnionCommunity also advertises social media, market and cloud services that are in development.

Screenshot of page on OnionCommunity that is very similar to Winzen's former layout

While it took several weeks for users of Daniel's services to recover what data was available and scrambled to figure out where to congregate and how to communicate, the community seems

more resolved than ever to continue with or without Daniel's support and the darknet itself continued to grow throughout the second-half of March, while Winzen was offline.

In fact, **since March 11th 2020, DarkOwl has observed an average growth of 387 new domains per day across the entire darknet**.

Stay tuned for more updates as we continue to track darknet trends and post updates on our blog.